AGENCY OF HUMAN SERVICES

AHS Program Management Standard

Jack Green

10/9/2013

The purpose of this procedure is to facilitate the implementation of the Vermont Health VHC's security control requirements for the Program Management (PM-2, PM-3, PM-4, PM-5, PM-6, PM-7, PM-8, PM-9, PM-10, PM-11) Controls.

Revision History

Date	Version	Description	Author
	.99	Procedures received from HI and reviewed by Referentia	
10/9/2013	3.0	Reviewed and adapted to VHC business processes	Jack Green

PURPOSE/STANDARD STATEMENT:

The purpose of this procedure is to facilitate the implementation of the Vermont Health VHC's (VHC) security control requirements for the Program Management (PM-2, PM-3, PM-4, PM-5, PM-6, PM-7, PM-8, PM-9, PM-10, PM-11) Controls.

The information systems covered in this procedure document contain but are not limited to the following:

- VHC website
- VHC Portal
- VHC workstations and mobile phones
- Network Accounts
- E-Mail accounts

SCOPE

The scope of this standard includes the VHC and its constituent systems only

STANDARD

Chief Information Security Officer

1. The DII CIO shall appoint a chief information security officer with the mission and resources to coordinate the development, implementation, and maintenance of a VHC-wide information security program. These activities are completed by the Agency of Human Services Information Security Director (AHSISD).

Security Program Plan

2. The AHS ISD shall develop, disseminate, review (at least annually), and update as needed an organizational security program plan that contains, at a minimum:
    a. An overview of the requirements for the security program and a description of the security program management controls and common controls in place or planned for meeting those requirements.
    b. Sufficient information about the program management controls and common controls (including specification of parameters for any assignment and selection operations either explicitly or by reference) to enable an implementation that is unambiguously compliant with the intent of the plan and a determination of the risk to be incurred if the plan is implemented as intended.

c. Defined roles, responsibilities, management commitment, coordination among organizational entities, and compliance.
d. Approval by a senior official with responsibility and accountability for the risk being incurred to organizational operations (including mission, functions, image, and reputation), organizational assets, individuals, and other organizations.

Information Security Resources

3. VHC Business Owners shall, at a minimum:
    a. Ensure that all capital planning and investment requests include the resources needed to implement the information security program and documents all exceptions to this requirement.
    b. Record the resources required.

Plan of Action and Milestones Process

4. VHC Business Owners shall implement the AHS ISD-specified process for ensuring that plans of action and milestones for the security program and the associated organizational information systems are maintained and document the remedial information security actions (from identification of needed action through assessment of implementation) to mitigate risk to organizational operations and assets, individuals and other organizations.

Information System Inventory

5. VHC shall develop and maintain an inventory of information systems as directed by the AHS ISD.

Information Security Measures Of Performance

6. VHC shall develop, monitor, and report on the results of information security measures of performance as directed by the AHS ISD.

Enterprise Architecture

7. VHC enterprise architecture shall be developed, and maintained, by the AHS ISD; with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals and other organizations.
8. Contractors of VHC and Business Partners shall design, develop, implement, and operate VHC related information systems in accordance with the VHC enterprise architecture.

Critical Infrastructure Plan

9. Business Owners shall address information security issues in the development, documentation, and updating of a critical infrastructure and key resources protection plan.

Risk Management Strategy

10. VHC shall:
    a. Develop a comprehensive strategy to manage risk to organizational operations and assets, individuals and other organizations associated with the operation and use of information systems.
    b. Implement that strategy consistently across the organization.

Security Authorization Process

11. VHC shall:
    a. Manage (i.e., document, track, and report) the security state of organizational information systems through the security authorization processes.
    b. Fully integrate the security authorization processes into an organization-wide risk management program.

Mission/Business Process Definition

12. VHC shall:
    a. Define mission/business processes with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals and other organizations.
    b. Determine information protection needs from the defined mission/business processes and revise the processes as necessary, until appropriate protection is obtained.

IMPORTANT INFORMATION

These procedures can be found at http://dvha-intra.ahs.state.vt.us/policies-protocols/InfoSec